

REMARKS

In view of the foregoing amendments and following remarks, Applicant respectfully requests reconsideration of the present application. At the time of the outstanding Office Action, August 6, 2008, claims 1, 3-8, 10-15, 17-21, and 23-32 were pending. By this response claims 1, 3-8, 10-15, 17-21, 23-30 and 32 are amended, and claim 31 is canceled. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

The Prior Art Rejection:

In the Office Action, claims 1, 3-8, 10-15, 17-21, 23-30, and 32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,175,917 to Arrow *et al.* (hereinafter “Arrow”) in view of U.S. Patent Application Publication 2001/0042201 to Yamaguchi *et al.* (hereinafter “Yamaguchi”). Applicant respectfully traverses this rejection for at least the following reasons.

The instant claims deal with managing IPsec communication sessions with an IPsec setting apparatus, such that authentication and security parameter setting occurs on the IPsec setting apparatus rather than on the remote machines utilizing the network security protocol.

Consider claim 1, which as amended recites, in part:

A network comprising:

...
an IPsec setting apparatus, which manages IPsec settings of the IPsec processing apparatuses,
wherein in response to **receiving a request from a first IP processing apparatus to communicate with a second IPsec processing apparatus**, the IPsec setting apparatus **transmits a request** to the second IPsec processing apparatus **and upon receiving a reply to the request** from the second IPsec processing apparatus the IPsec setting apparatus **transmits a common encryption key to the first and second IPsec process apparatuses to be used to encrypt and authenticate IPsec communications** between the first and second process apparatuses.

The cited art does not teach or suggest this material. Arrow makes no mention of a first VPN unit (Virtual Private Network unit) issuing a requesting to communicate with a second VPN unit, much less a first a VPN unit issuing a request to the VPN management station to communicate

with a second VPN unit. Arrow merely discusses that upon receiving an outbound packet a VPN unit determines whether or not the source and destination of the packet are both members of the same Virtual Private Network (VPN), and if both are members of the same VPN, then the VPN unit processes the packet in accordance with the rules identified by a lookup table maintained by the VPN unit. (Col. 7, line 12 – Col. 8 line 3 and Fig. 2.) Thus, the VPN units of Arrow do not make requests to the VPN management unit in order to communicate with other VPN units, unlike the instant claims in which the IPsec processing apparatuses make requests to communicate with other IPsec processing apparatuses to the IPsec setting apparatus in order to receive the encryption key to be used during the communication.

Furthermore, since Arrow does not disclose the VPN management station receiving, from a first VPN unit, a request to communicate with a second VPN unit in order for both units to receive an encryption key, Arrow does not disclose, in response to the request, an IPsec setting apparatus transmitting a request to the second IPsec processing apparatus, nor disclose upon receiving a reply to the request transmitted to the second IPsec processing apparatus, transmitting a common encryption key to the first and second IPsec processing apparatuses to be used in the communication between the first and second apparatuses.

Nor are the deficiencies of Arrow cured by Yamaguchi. Yamaguchi merely discusses a VPN system which uses routers having an IPsec function, (¶ 0008, lines 1-4) wherein the level of security of a communication corresponds to a user and a destination. (¶ 0037, lines 1-13.) Yamaguchi does not teach or discuss an IPsec setting apparatus receiving a request from a first IPsec processing apparatus to communicate with a second IPsec processing apparatus, and in response to the request the IPsec setting apparatus transmits a request to the second IPsec processing apparatus, and further in response to a reply from the second IPsec processing apparatus, the IPsec setting apparatus transmits a common encryption key to the first and second IPsec processing apparatuses. The instant claims provide the advantage preventing inconsistency of settings among IPsec processing apparatuses during communication and reductions in communication start times and operational loads for IPsec processing apparatuses. (¶¶ 0016, 0032, 0034-0037, 0042) Thus, for at least the foregoing reasons, claim 1 defines over the cited art.

Concerning claim 8, claim 8 recites an IPsec setting apparatus that receives from a first IPsec processing apparatus a request to communicate with a second IPsec processing apparatus and in response the IPsec setting apparatus manages the IPsec policies to be used in communication

between the first and second IPsec processing apparatuses. As already discussed the cited art does not teach or suggest an IPsec setting apparatus receiving a request from a first IPsec processing apparatus to communicate with a second IPsec processing apparatus. Thus, the cited art also does not teach or suggest in response to the request the IPsec setting apparatus managing the IPsec policies between the IPsec processing apparatuses. Thus, for at least the foregoing reasons, claim 8 defines over the cited art.

Concerning claim 15, claim 15 recites an IPsec processing apparatus that transmits to an IPsec setting apparatus a request to communicate with another IPsec processing apparatus and in response to the request the IPsec processing apparatus receives from the IPsec setting apparatus the IPsec and setting to be applied to the communications with the other IPsec processing apparatus. As already discussed the cited art does not teach or suggest an IPsec setting apparatus receiving a request from a first IPsec processing apparatus to communicate with a second IPsec processing apparatus. Consequently, the cited art also does not teach or suggest in response to a request from a first IPsec processing apparatus, an IPsec setting apparatus transmitting an IPsec or a setting to the requesting IPsec processing apparatus. Thus, for at least the foregoing reasons, claim 15 defines over the cited art.

Concerning claim 21, claim 21 is a method claim and recites receiving from a first IPsec processing apparatus a request to communicate with a second IPsec apparatus, in response to the received request sending a request to the second IPsec apparatus and in response to a reply from the second apparatus generating and transmitting IPsec setting parameters to the first and second IPsec processing apparatuses. As already discussed the cited art does not teach or suggest receiving a request from a first IPsec processing apparatus to communicate with a second IPsec processing apparatus. Consequently, the cited art also does not teach or suggest in response to the received request sending a request to the second IPsec apparatus nor in response to a reply from the second IPsec processing apparatus generating and transmitting to the first and second IPsec processing apparatuses IPsec setting parameters. Thus, for at least the foregoing reasons claim 21 defines over the cited art.

Claims 3-7, 10-14, 17-20, 23-30 and 32 depend from claims 1, 8, 15 and 21, respectively, and therefore also define patentable subject matter. Accordingly Applicant respectfully requests allowance of the instant claims.

CONCLUSION


Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by the credit card payment instructions in EFS-Web being incorrect or absent, resulting in a rejected or incorrect credit card transaction, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date 10/28/2008

By 

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 945-6014
Facsimile: (202) 672-5399

George C. Beck
Attorney for Applicant
Registration No. 38,072